Audit Report

OFFICE OF THE INSPECTOR GENERAL

ALLEGED MISUSE OF "SGT SECURITY" COMMERCIAL SOFTWARE

Report Number 92-092   May 15, 1992

20000602 126

Department of Defense

AQI00-08-2603

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

REPORT
NO. 92-092   May 15, 1992

MEMORANDUM FOR ASSISTANT SECRETARY OF THE AIR FORCE
                  (FINANCIAL MANAGEMENT AND COMPTROLLER)

SUBJECT: Audit Report on the Alleged Misuse of "SGT
           Security" Commercial Software (Project No.
           2RF-5004.01)

Introduction

      We made the audit in response to a request from Senator
William V. Roth, Jr., to determine the validity of allegations
that a commercial software program, "SGT Security," was misused
by the U.S. Air Force 7th Communications Group (7CG) in violation
of U.S. copyright laws.   The audit was conducted from December
1991 through February 1992 as a part of our audit of Controls
Over Copyrighted Computer Software (Project No. 2RF-5004).   "SGT
Security" is produced by Pike Creek Computer Company (the
Company) and marketed by the Kaleidoscope Company.   The program
is designed to erase previously stored data from computer disks.
"SGT Security" is advertised as capable of erasing all types of
sensitive and secure files and is marketed as a means of
declassifying computer disks.   The software is normally licensed
for 4 years, and each copy is restricted for use on only
one microcomputer.

      Since individuals can easily make copies of most software,
we cannot be assured that illegal copies of "SGT Security" were
not made.   However, the audit disclosed no evidence of illegal
use or dissemination of "SGT Security" within the 7CG or other
activities supported by the 7CG.   During the audit, 7CG officials
initiated procedures to control and account for copyrighted
commercial software.

Scope of Review

      The audit focused on allegations that the 7CG misused "SGT
Security" software by copying and using it without permission
from the Company.   We interviewed personnel within 7CG and other
activities that knew of "SGT Security."   We also reviewed
declassification procedures and required documentation within the
7CG.   Based on discussions with the Company, we determined that
7CG's use of "SGT Security" could not be determined by scanning
computer hard drives, if it had been used as alleged.

We reviewed documentation provided by the National Computer Security Center (NCSC) regarding its evaluation of "SGT Security" and its subsequent removal from the NCSC's Evaluated Product List. We also reviewed documentation from the Air Force Cryptologic Support Center concerning contacts with the Company and assessments of "SGT Security" and other computer software designed to erase computer disks. In addition, we contacted the Company on several occasions to clarify and obtain additional information to support its allegation. In an attempt to confirm or refute the allegation, we also contacted each person the Company identified to us as having knowledge of the use of "SGT Security" within the 7CG.

Our review did not include an assessment of the capabilities of "SGT Security," and we offer no opinion on its utility. Since the NCSC no longer evaluates software products designed to overwrite and sanitize computer media, an opinion concerning the usefulness of "SGT Security" was not provided.

The audit was made in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General, DoD. The audit included such tests of internal controls as were considered necessary. Activities visited or contacted are shown in Enclosure 2.

Internal Controls

Procedural weaknesses over the receipt and disposal of vendor-supplied computer software protected by U.S. copyright laws and licensing agreements will be determined in the overall audit of Controls Over Copyrighted Computer Software and will be reported on a DoD-wide basis.

Prior Audit Coverage

There has been no prior review or audit coverage concerning the specific allegation discussed in this report. Both the Army and the Air Force audit agencies have performed general audit coverage of controls and accountability over microcomputer software. That coverage will be discussed in the summary report of our audit of Controls Over Copyrighted Computer Software (Project No. 2RF-5004.)

Background

The 7CG is located in the Pentagon and provides communications and computer systems support to Headquarters, Department of the Air Force; the Joint Staff; and staff offices

2

within the Office of the Secretary of Defense. Part of the 7CG's responsibilities include providing computer security and software application support for about 7,000 small computers within the Pentagon.

The NCSC published an evaluation of "SGT Security" (Version 4A) in July 1987 and placed it on its Evaluated Products List (EPL). The evaluation stated that "SGT Security" applied required overwrite procedures to clear internal magnetic media within specific constraints, (e.g., the product was effective on specific models of computers produced by the International Business Machines Corporation). In 1989, a potential problem with Version 4A was reported. According to the NCSC, the Company corrected the deficiency in Version 4A.1. "SGT Security" remained on the EPL until January 1990 to notify users of the potential problem in version 4A and of the vendor's subsequent correction of the problem in Version 4A.1. "SGT Security" was removed from the EPL because the NCSC discontinued evaluating products designed to erase computer media.

The Company contacted Senator Roth in August 1991, after learning from the <u>Federal Computer Week</u> and other unnamed sources that the Air Force misused "SGT Security." Articles in the <u>Federal Computer Week</u> indicated that a technical sergeant within the 7CG received an "Unsung Hero of Computer Security" award.[1] The award was given to the sergeant because of his discovery that "SGT Security" did not completely erase classified data from computer hard disks and because of his proposed "workable solution" to combine "SGT Security" with another utility program to ensure that computer hard disks were completely erased. The award nomination stated that the discovery saved the Air Force thousands of dollars, since hard disks containing classified data could now be erased and reutilized. However, that same individual was awarded the Air Force Achievement Medal on October 10, 1990. The citation for that award stated only that the sergeant discovered a flaw in a commercial computer security software program. According to the citation, that discovery avoided possible compromise of classified information. The official citation made no mention of the proposed solution described in the Unsung Hero award.

If "SGT Security" was combined and used with another utility program or used by itself to erase computer disks, a violation of U.S. copyright laws could have occurred, since the 7CG did not

---

1 The award was jointly sponsored by the <u>Federal Computer Week</u> and the Open Systems Conference Board, a non-profit organization not connected with the Government.

have a license to use "SGT Security." The Defense Federal Acquisition Regulation Supplement 252.227-7013 prohibits unauthorized distribution or copying of commercially-developed software without written consent from the supplier.

Discussion

There was no evidence that anyone within or connected with the 7CG used "SGT Security" in an illegal or improper manner.

Evaluation of "SGT Security". On June 7, 1988, the Company provided a demonstration copy of "SGT Security" to the 7CG for evaluation. The Company and the 7CG made an informal verbal agreement for the 7CG to evaluate "SGT Security" to determine whether the software would meet requirements. The person assigned to evaluate the software found that "SGT Security" could erase files on Zenith computers commonly used within the 7CG; however, "SGT Security" did not erase the file directories. This deficiency was discussed and confirmed with the Company in subsequent meetings. Contact between the Company and 7CG was discontinued in the fall of 1988.

The Company alleged that during a meeting in early 1989, the sergeant, who evaluated "SGT Security," returned a copy of the software diskette rather than the original and did not return the manual. The Company stated that it did not examine the disk that was returned by the 7CG until the article that appeared in Federal Computer Week was brought to its attention in 1991. Personnel at the 7CG had no recollection of the meeting and stated the entire "SGT Security" package was mailed to the Company along with the only backup diskette made. The 7CG did not have formal procedures for receipt or return of commercial software and could produce no mailing record to support its claim. Neither version of the circumstances surrounding the return of the software could be verified.

The Air Force Cryptologic Support Center (AFCSC) assessed Version 4A (the same version provided to the 7CG) of "SGT Security" in May 1988 and recommended in an internal report that it should not be used until the vendor made certain modifications. On June 21, 1988, personnel from AFCSC discussed problems found in "SGT Security" with the Company's marketing agent. Based on that discussion, the company was apparently aware of deficiencies with "SGT Security" during the same time period that the software was being marketed.

Beginning in November 1988, the AFCSC published assessments of other software, such as "Killdisk" (an Air Force owned product produced by Pan Am World Services) and Norton Utilities'

4

"Wipedisk." The AFCSC's assessments stated that the software could effectively overwrite magnetic disks when tested on specific hardware and software.

Proposal to Use "SGT Security". The sergeant within the 7CG who discovered that the software did not completely erase all information on computer disks, proposed in an August 3, 1988, Memorandum for the Record that "SGT Security" be used together with "Wipedisk" to declassify computer disks. According to the proposal, this interim procedure was recommended to declassify disks until another software program, being evaluated by the AFCSC, could be completed. Although the proposal required the approval of the 7CG Director of Security, there was no documentation to show whether the proposal had been approved within or outside the 7CG. We found no evidence that anyone within the 7CG had ever used the procedure in the proposal, seen it used, or knew of anyone who had used it. We discussed our findings with the 7CG Director of Security (the Director) who wrote the "Unsung Hero" nomination. He stated he wrote the award nomination and submitted it to Federal Computer Week without assistance or review by anyone within the 7CG, since there were no established procedures within the 7CG for review of nominations made for non-governmental awards. The Director did not have technical knowledge of computer operations. He was informed that "SGT Security" did not completely erase computer disks but that it could be used in conjunction with "Wipedisk" to declassify computer disks. The Director stated that he was not told that "SGT Security" had been used; he assumed it had been used. The Director did not know whether any funds were actually saved, but the proposal could have saved thousands of dollars if it was used. He felt the "Unsung Hero" award was deserved, because the nominee had avoided significant problems for the Government by discovering a fault in the software, which was previously considered capable of totally erasing computer disks.

Erasure of Classified Data. Erasure of classified data stored on computers with operating systems compatible with "SGT Security" frequently was not required throughout the 7CG. Due to the infrequency of declassifying computer media, Computer System Security Officers outside the Security Directorate were not aware of 7CG policies and procedures for documenting the declassification of computer disks. Only one office within 7CG routinely declassified data stored on computer hard disks. According to computer personnel performing the operation, the computer hard disks were erased using Norton Utilities' "Wipedisk." No other method was used. Although the erasures were not properly documented in accordance with 7CG "Declassification Procedures," May 13, 1992, there was no indication "SGT Security" was used.

The audit identified only one activity associated with the 7CG that had used "SGT Security" to declassify computer disks. The office of the Assistant Secretary of Defense (Program Analysis and Evaluation) (ASD[PA&E]) purchased a license to use

25 copies of "SGT Security" in November 1988. Since the 7CG supports ASD(PA&E) data automation requirements, an officer assigned to the 7CG acted as custodian for the software received. Based on discussions with the custodian and a March 17, 1991, memorandum to Division Security Officers in ASD(PA&E), we concluded that the software was issued to at least 14 personnel within ASD(PA&E) and at least 1 individual within 7CG who supported ASD(PA&E). In 1990, a new custodian was assigned. The new custodian stated that during 1990, he was advised by security personnel that the software should not be used. As a result, he discarded "SGT Security" disks, manuals, and records of individuals that may have used the software. However, the custodian neither retrieved the disks that were distributed nor notified the users that it should not be used. We contacted individuals in the offices that may have received the software and found one copy of "SGT Security" on hand. The copy was not in use.

Management Comments

A draft of this report was provided to the Assistant Secretary of the Air Force (Financial Management and Comptroller) for comment on March 27, 1992. Department of the Air Force comments on the draft report, dated April 30, 1992, concurred with the audit findings (see Enclosure 1).

The courtesies extended to our staff are appreciated. Please contact Mr. Harrell D. Spoons at (703) 693-0101 (DSN 223-0101) or Mr. Marvin L. Peek at (703) 693-0104 (DSN 223-0104) if you have any questions concerning this report. Distribution of this report is shown in Enclosure 3.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Enclosures

cc:
Secretary of the Air Force
Under Secretary of Defense for Policy
Assistant Secretary of Defense (Command, Control,
  Communications and Intelligence)
Assistant Secretary of Defense (Program Analysis
  and Evaluation)

DEPARTMENT OF THE AIR FORCE
7TH COMMUNICATIONS GROUP
WASHINGTON DC 20330-6345

3 0 APR 1992

REPLY TO
ATTN OF: CC

SUBJECT: DOD (IG) Draft Audit Report on the Alleged Misuse of "SGT SECURITY"
Commercial Software (Project No. 2RF- 5004.01)

TO: AF/SCXX

1. This is in reply to the memorandum for Assistant Secretary of the Air Force
(Financial Management and Comptroller) requesting comments to the subject
report.

2. We concur with the findings in the report. Based on discussions during the
audit, we published two regulations, 7CGR 700-10, Small Computer Hardware and
Software Management, and a supplement to AFR 900-20, Special Trophies and
Awards, to further improve internal management. These revised requirements will
clarify 7CG procedures to better control both contractor provided test software
and the Group awards program.

3. The 7CG point of contact is Major Chambers, 7CG/DS, (703) 697-7429.

WILLIAM B. RANKIN, Colonel, USAF
Commander

ENCLOSURE 1

ACTIVITIES VISITED OR CONTACTED

Office of the Secretary of Defense

Assistant Secretary of Defense (Program Analysis
and Evaluation)

Department of the Air Force

7th Communications Group
Air Force Cryptologic Support Center, Air Force Intelligence
Command

Other Defense Activities

National Computer Security Center

Non-Government Activities

Pike Creek Computer Company
Kaleidoscope Company

REPORT DISTRIBUTION

Office of the Secretary of Defense

Under Secretary of Defense for Policy
Assistant Secretary of Defense (Command, Control,
  Communications and Intelligence)
Assistant Secretary of Defense (Program Analysis and
  Evaluation
Assistant Secretary of Defense (Public Affairs)
Comptroller of the Department of Defense

Department of the Air Force

Secretary of the Air Force
Assistant Secretary of the Air Force (Financial Management
  and Comptroller)
Auditor General, Air Force Audit Agency
Air Force Cryptologic Support Center, Air Force Intelligence
  Command

Other Defense Activities

Director, National Security Agency/Central Security Service
Inspector General, Defense Intelligence Agency
Defense Logistics Studies Information Exchange
National Computer Security Center

Non-DoD Activities

Office of Management and Budget
U.S. General Accounting Office
  NSIAD Technical Information Center
Library of Congress
  Copyright Office
  Inspector General

Congressional Committees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Committee on the Judiciary
Senate Subcommittee on Patents, Copyrights, and Trademarks,
  Committee on the Judiciary
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations

REPORT DISTRIBUTION (continued)

Congressional Committees (Cont'd):

House Committee on Armed Services
House Subcommittee on Legislation and National Security,
  Committee on Government Operations
House Subcommittee on Government Information, Justice, and
  Agriculture, Committee on Government Operations
House Committee on the Judiciary
House Subcommittee on Courts, Intellectual Property, and the
  Administration of Justice, Committee on the Judiciary
House Committee on Science, Space, and Technology
House Subcommittee on Science, Research, and Technology,
  Committee on Science, Space, and Technology
House Permanent Select Committee on Intelligence
House Subcommittee on Oversight and Evaluation, Permanent
  Select Committee on Intelligence